Federal Electronic Commerce Coalition

"Providing a consolidated voice from industry to government"

FECC DOD/Industry Working Group

Final Report
December 11, 2000

Impact Assessment of DOD's Public Key Infrastructure (PKI) Policy

Federal Electronic Commerce Coalition

"Providing a consolidated voice from industry to government"

TABLE OF CONTENTS

Federal Electronic Commerce Coalition (FECC)
DOD/Industry Working Group
For
Impact Assessment of DOD's PKI Policy

December 11, 2000

EXECUTIVE SUMMARY

The FECC, working primarily through AFCEA, AFEI, IAC, and ICH member companies, has at the request of the Department of Defense (DOD) (attachment 1), led an Industry review of the DOD Policy for Public Key Infrastructure (attachment 2). The Industry Working Group (IWG) thanks the DOD CIO's Office for the opportunity to provide Industry input in this very important area and congratulates the Department on its openness and willingness to accept and consider the IWG's recommendations. The IWG also commends the DOD for its aggressiveness in forging ahead towards solutions in the area of PKI, authentication and information assurance.

The IWG impact assessment of the DOD PKI policy, followed the guidelines presented to the IWG in the DOD request and White Paper entitled "DOD PKI Policy Impact Assessment" (attachment 1).

The current DOD PKI policy (and subsequent implementation objectives) supports and makes fundamental, the premise that DOD operational communication networks must be protected from both outside and inside attack and disruption of a malicious nature. Consequently, it is the IWG's considered opinion that the policy has been formulated to address the highest level of security and protection within the PKI domain, class 4 (four).

The current policy has not taken into account varying functional operational requirements, applications, processes or policies as they pertain to the day-to- day business operations within DOD. Likewise the policy does not address, or take into consideration, the burgeoning e-Business environment that DOD is developing with its

As was previously stated, the current DOD Policy focuses on the protection of networks and does not consider end-user applications. Given these parameters, the IWG assessment focused on the business environment in which functional domains must operate; the cost and impact on Industry or others who must interact with the DOD from without; and the trends of how business will be conducted in the "New Economy". The assessment also took into account emerging Commercial Practices and current solutions being proposed that are COTS based or lend themselves to an open, interoperable architecture.

The IWG assessment focused on the DOD e-Business operations and does not apply to the operational environment of Command and Control or Intelligence. The assessment considered work outside of the DOD, concentrating in the areas of PKI infrastructure, interoperability and policy at the Federal Government level as well as the emerging business practices and policies in the commercial market. It is also important to note that e-Business transactions were defined as "all electronic transaction required in conducting operations/business processes between two entities". Thus, the IWG assessment did not just limit itself to transactions pertaining only to contracting/procurement or their inherent issues. Other transactions, such as simple e-mail, medical and personnel records transfer, financial transactions, technical document transfers, legal document transactions, travel documents or the myriad of other business processes that transpire daily in commercial and government entities, were all part of the IWG considerations.

Therefore, because of the scope of transactions described above, the IWG strongly endorses the work that has been accomplished by the Federal PKI Steering Committee in developing and testing the Federal PKI Bridge Certification Authority and its efforts to implement that solution by the end of calendar year 2000. However, there is considerable consternation from Industry, as to the lack of inclusion of the Federal PKI Bridge in the DOD policy, current DOD PKI solution, and the prescribed direction for the DOD. The IWG understands that there is a DOD PKI Bridge Demonstration project that "mirrors" the Federal PKI Bridge effort, but we could find no factual evidence that the DOD Demonstration is more than a simple "Demonstration". In other words, we could find no DOD commitment to an "operational life" beyond its current "Demonstration" configuration. Thus, we had to conclude that the DOD PKI Bridge will not end up as part of the DOD Global Information Grid (GIG) as a viable solution for conducting secure

Additionally, serious consideration should be given to NOT precluding Class 2 level certs in certain transactional or communication instances. If not, DOD's Industry trading partners and others, including retirees, dependents and other government and non-government counterparts, who will have a need to access and communicate with those inside the enclaves of the DOD, will be faced with implementing a solution that does not have a strong business foundation and will negatively impact the cost and effectiveness of e-Business within the Department.

The IWG also recommends that DOD immediately initiate efforts, within their various functional communities, to define their business processes and transactions that may require varying levels of PKI. The IWG believes that these transactions will fall into various functional "bands" so that different levels of PKI solutions apply to each band. The IWG is prepared to provide members, with the requisite functional expertise, to work with the various DOD functional communities to insure a continuity of operations between DOD and the commercial environment when PKI applications are deployed. This work requires investigation of different levels of authentication requirements based on applications, business processes and business cases. If DOD considers this an option, then DOD guidance is necessary for dealing with the varying cert levels.

The IWG is also prepared to discuss the legal issues emanating from the current policy guidance, and await specific direction in this area. Even though the group has been formed to deal with a seemingly technical set of issues, the IWG accepts the fact that continuing effort must encompass the strategy and direction of the overall DOD e-Business program and the functional communities that constitute that program. This would include liability and potential litigation issues.

In developing the DOD PKI impact assessment, the IWG was organized into four sub-groups. These groups addressed specific aspects of the effort. They were as follows:

1) Emerging Commercial Practices
2) Legal Issues
3) Technical Issues
4) Policy

Emerging Commercial Practices in PKI

Work Group Participants

Keren Cummins, Chair, Digital Signature Trust Co.
Joshua Icore, Secure Computing
Hays McCormick, Interoperability Clearinghouse
Beverly Nitkowski, Dyncorp
David Papas, Secure Computing
Johnny Sumners, Tidepoint

Background

The DOD ASD C3I August 12 Policy Memo calls for DOD to evolve to Class 4 certificates for all environments and applications that employ public key technology. Migration for certain mission-critical components must be completed by December 31, 2003; for all other environments by December 31, 2006. While the Memo describes the strategy as one of enabling security services at multiple levels of assurance, ultimately all the focus of the document is upon the Target Class 4 environment for all Components.

The Deputy CIO and the Director of Defense Reform have asked for an impact statement from industry. This FECC working paper is intended to provide background on emerging commercial practices in PKI and how these practices might impact upon, benefit, or conflict with the August 12 policy memo.

Problem

Different functions require different levels of assurance and the higher the assurance level the higher the cost of implementation. The very high level of assurance afforded by a Class 4 PKI seems reasonable for core DOD functions and for ensuring the integrity of

The commercial sector is undergoing its own evolutionary process in the use of PKI. This process is taking different paths in different commercial domains, with a "domain" defined as encompassing areas like B2B (EC/EB), healthcare, personnel/retirement, financial services, logistics. It appears that security models different from DOD's (and often less costly) are emerging, are evolving into best practices, and will eventually dominate different commercial domains. The drivers for security and privacy are different for each domain and are different from DOD's fundamental drivers for Information Assurance.

Rather than dictating its own security procedures and infrastructure to each of these domains, DOD may be better served by (1) individually evaluating its security requirements for activities in these domains, and (2) where appropriate, accommodating its business processes in certain functional areas to the emerging commercial standards for those domains. This paper does not attempt to address what the appropriate policies should be for specific DOD activities but only to highlight the trust approaches that are emerging for similar activities in the private sector.

New Opportunities

One challenge facing DOD, or any PKI-enabled enterprise that touches multiple commercial domains, is how to interpret and accept certificates issued by other organizations and under different policies. Because this is very difficult, the default response has been to choose not to accept certificates issued by other entities at all.

However, two developments have made the prospect of interoperating with other PKI's more realistic. The development of the Federal Bridge CA offers a *technical* mechanism for DOD to accept certificates originated outside DOD, at various Class levels. And the emergence of broad community-of-interest PKI's (i.e., a PKI serving a large community of separate enterprises for e-commerce purposes) in the commercial sector similarly offers a simplified mechanism for the DOD PKI to accept certificates from a major domain with which it does business. The emergence of these changes in the technical and business environment suggests that DOD should be prepared from a *policy* standpoint (at a DOD and at a functional level) to consider these options.

As a result, either of these (Federal Bridge CA, COI PKI's) may make the acceptance of additional levels or classes of certificates technically feasible for some DOD applications that extend outside the secure perimeter. This will greatly lower the cost of participation by those communities (and hence, likelihood of participation) while allowing DOD to move them to a greater level of security/efficiency than that at which they currently operate.

It is important to note that the trust standards that are emerging commercially and in G2B

(1) tend to be different for different domains; and
(2) do not necessarily map neatly into DOD named Classes, e.g., Class 2, 3 or 4.

Rather, the trust standards are uniquely designed to support the categories of business processes required by those domains (health care information, procurement information, etc.) and in many cases involve elements not contemplated by the DOD Class definitions. As a result, a simple direct mapping of these commercial trust standards to DOD classes does not yield good information about the true strength of each approach.

Discussion of emerging PKI communities of interest in commercial sector:

Following are some examples from both the commercial sector and from the G2B/G2C sectors. These are not comprehensive but are intended to illustrate the degree to which COI's tailor their security practices to the needs of the community/transactions being supported, and the degree to which they do or do not map to the current DOD classification system (e.g., Class 2, Class 3, Class 4). It is worth noting that several of the COI's requiring higher levels of assurance have defined policies similar to DOD's recently proposed Class 3 + hardware assurance level.

Financial Services, EC/EB, Logistics

TrustID® (B2B, B2C)

- TrustID certificates are issued to banking customers in a setting where the bank has enjoyed an ongoing relationship with the customer. The certificate is issued through an online interaction with an out-of-band component to a well-known customer with an existing electronic relationship with the bank. Accordingly, it maps to DOD Class 2 but is more comparable to Class 3 or 3+
- Key storage is typically in the browser, or optionally on a smart card.

Identrus (B2B)

Description: The Identrus infrastructure was created for financial institutions, their corporate customers and security vendors to enable corporate trading partners to eliminate the time, cost and complexity of building trust relationships with counterparts around the world. The Identrus legal and technical infrastructure is based on a set of uniform system rules, contracts and business practices for comprehensive trust and risk management. Digital certificates are issued by participating financial institutions. Various vendor's CA products (tailored for Identrus) are supported. All parties exchange digital certificates.

- Certificates are issued to individuals at major corporate entities on the basis of in-person proofing; the CP also requires smart cards, but does not go as far as Class 4 in its technical requirements for those cards.
- Because of the in-person proofing and the use of smart cards, this is roughly comparable to a "Class 3+"

ACES Business Certificates (B2G)

Description: The Access Certificates for Electronic Services (ACES) program is designed to put digital certificates in the hands of businesses and individuals needing to conduct authenticated transactions with federal government agencies. ACES certificates are issued by any of three approved ACES vendors according to a GSA-developed certificate policy and provisions of the contract. The contract includes a number of specific security requirements not detailed in the CP.

- ACES Business certificates are issued using a combination of database checking about the company along with the submission of a "wet" signed document conveying

IECA Program (B2G)

Description: The Interim External Certification Authority (IECA) program was developed by DISA and NSA in coordination, to provide a mechanism for DOD's external trading partners to conduct secured transactions, particularly in support of procurement-related activities such as Wide Area Work Flow and Electronic Document Access. Certificates can be purchased by companies from any of four IECA vendors, who were approved after submission and approval of an MOA, their proposed IECA CPS, and supporting documentation.

- IECA certificates are issued to a business representative after the individual provides personal and professional information about the company he or she plans to represent. Information is submitted electronically as well as on a notarized and signed document conveying authority to represent the company, and is validated using third party databases. Wet signed documents are archived at the CA.
- Business certificates do not have a direct analog in the FBCA or DOD CPs. Because of the database checking and the submission of a signed and notarized document, this is roughly comparable to a Class 3+.
- IECA certificates are stored in the browser, or optionally on a smart card.

Healthcare

Healthcare Community PKI

Description: a suite of documents recently developed for a broadly-based healthcare PKI; the development process included at least one major company from each of the pharmaceutical, prescription, HMO, health care delivery, and insurance communities.

- Certificates issued under this CP are ***anonymous***; that is, there is nothing in the cert that tells you who it belongs to. The cert contains a unique ID tied to information in a database, and the relying party only gets the name (and related identity information) through the validation process. This approach provides

- There are three levels of individual certificates. While these are not strictly comparable to DOD Classes because of the additional privacy protections afforded here, a rough mapping is provided:
  - Consumers, employees: Certificates are issued using a browser-based, web enrollment process, with validation of supplied data from third party databases. There is also a two-factor authentication requirement at the application (Class 2++). Key storage for this and the next level typically takes place in the browser.
  - Consumers, employees: Includes all of the above elements, plus in-person registration with a financial or corporate notary (Class 3++)
  - Physicians: Includes all of the above but must be held on a smart card (Class 3+++ -- would easily qualify for Class 4 except for the FIPS 140-1 Level 3 requirements for Class 4 smart cards)
- There are two types of business certificates:
  - Administrator certificates – special authentication ties to the business entity, and must reside on smart card only
  - Server/device certificates
  - Participants need a web browser with 128-bit cipher strength and, to use the secure email feature, will need an email client that supports S/MIME and digital certificates.
- Policy review by a healthcare industry controlled policy advisory council
- The type of certificate acceptable is determined by the relying party

11.

California Medical Association (CMA)

Description: A PKI, provided by MEDePass (a subsidiary of CMA) designed to meet the needs of physicians for secure communications amongst themselves. MEDePass digital certificates are issued to both CMA member physicians and non-CMA member physicians, but not to non-physicians. MEDePass, Inc. is a member of MoHCA (Mobile Health Care Alliance) – an industry alliance dedicated to the development of standards and practices to ensure trusted mobile health care.

- CMA uses Colleague Referral, as follows: a physician subscribes to MEDePass, the physician identifies colleagues with whom he or she would like to communicate securely, and the physician refers colleagues by sending MEDePass a digitally signed email with the colleagues' names and email addresses or by filling out a referral form online. The County Medical Society may also give a referral.
- Referred physician is emailed a non-secure message from MEDePass with Subscriber Agreement (SA) and PIN number. The referred physician can either mail or fax the SA to MEDePass. Once the SA is received by MEDePass, an electronic message is sent to the physician with instructions on how to obtain their digital certificate. The PIN number sent with the SA is used to obtain the certificate. This maps approximately to a Class 2 implementation.
- Participants need a web browser with minimum128-bit cipher strength and an email system that supports S/MIME and digital certificates.

Personnel, Retirement Benefits

ACES individual certificates

Description: The ACES program is designed to put digital certificates in the hands of businesses and individuals needing to conduct authenticated transactions with federal government agencies. ACES certificates are issued by any of three approved ACES vendors according to a GSA-developed certificate policy and provisions of the contract. The contract includes a number of specific security requirements not detailed in the CP. ACES individual certificates are being deployed for use at numerous federal agencies for purposes ranging from access control (FEMA) to form signing and/or submission (SSA, VA, Education, EPA).

- ACES individual certificates are issued to an individual on the basis of personal information supplied online. That information is checked for consistency against numerous third-party databases, and, if satisfactory, an authorization code is mailed out-of-band via USPS to the individual's physical address of record. Using this

Conclusions/Recommendations

It is the opinion of the FECC PKI Emerging Commercial Practices Working Group that Class 4 assurance, in most cases, does not appear to be necessary for the protection of e-business transactions, and will in fact place an unnecessary burden, and in some cases (small and disadvantaged businesses) a hardship to achieve this aggressive goal. The approach that the Department is undertaking may in fact

- slow the adoption of PKI acceptance,
- reduce trading partner participation,
- create an excessive and difficult infrastructure to manage and maintain,
- drive excessive implementation costs and, possibly
- diminish overall protection of sensitive information.

Industry is developing suites of practices carefully tailored to different domains of transactions. These appear to represent more cost-effective, more readily deployable and acceptable, and sufficiently secure alternatives to DOD's currently promulgated Class 4 approach. The emergence of consolidated industry groups, through either bridge technology or through the development of cooperating communities of interest, makes it feasible for DOD to consider interoperation with these industry sectors on more flexible terms. These can include DOD, or a functional area within DOD:

(1) Choosing to directly accept certificates from an external bridge or community of interest after determination that it meets the requirements of the application domain of interest; or,

(2) Encouraging an external bridge or community of interest to apply for acceptance by the Federal Bridge CA and be mapped into the FBCA CP.

The first option provides maximum flexibility for DOD to accommodate trust models that do not map well to BCA or DOD classes, i.e., those referred to above as "2+" or "3+," but it leaves the onus with DOD to conduct these evaluations. The second option has the benefit of passing the work of policy mapping to the FBCA, but will tend to evaluate some strong trust models as belonging in an inappropriately low trust class (i.e., a 3++ trust model will tend to evaluate as a "3", no matter how much stronger it actually is). Also, it is not clear at what time in the future the FBCA will evaluate applications from non-Federal entities.

A mechanism by which DOD can effect this new approach is to develop relying party policies tailored for the domain with which DOD intends to interact. Relying party policies would be developed if a DOD review and evaluation of dominant commercial practices serving that domain suggested that these practices meet DOD's assurance requirements. The relying party policy would spell out a set of minimum standards that DOD would require in order to accept externally-issued certificates in support of transactions in that domain (e.g., healthcare). Such a policy could include specific liability provisions as well as specifications for identification and authentication, and key storage. Clearly, the results of this approach can be made more effective if DOD becomes a participant in the discussions, as various commercial domains develop their policy practices and procedures.

LEGAL ISSUES IN PKI

CO-CHAIRS:
CHRISTOPHER YUKINS, ESQ., HOLLAND & KNIGHT LLP
RICHARD VACURA, ESQ., PIPER MARBURY RUDNICK & WOLFE LLP

The Public Key Infrastructure (PKI) Working Group was asked to comment upon the Department of Defense (DoD) initiative to implement secure electronic business (e-business). Legal issues comprise one important part of that initiative; this report addresses some of those legal issues.

Introduction to PKI

PKI is a system of public key cryptography combined with an infrastructure that is designed to provide a level of security for communicated and stored electronic information. Public key cryptography uses an algorithm to provide different but mathematically related keys, one for creating a digital signature or encrypting data, and another key for verifying a digital signature or decrypting data. When using PKI, one of the keys in the pair is kept private by the user while the other is made public (through a third-party "Certification Authority") and is shared with the computer on the other end of the information exchange transaction.

A PKI system provides parties to an electronic business transaction information attributes that are critical to create a legally binding transaction, including authentication (verifying and ensuring identity), integrity (protection of the information from unauthorized and undetected modification), and non-repudiation (associates a party with data such that it cannot deny the association nor claim modifications were made to the data), as well as confidentiality (protection of the information from unauthorized disclosure).

PKI thus plays a central role in electronic commerce, and will likely

Legal Milestones in Government's Implementation of E-Business

A key milestone in the federal government's move to e-business was the Government Paperwork Elimination Act (GPEA), Public Law No. 105-277, Title XVII (Oct. 21, 1998). GPEA requires federal agencies to implement e-government, including electronic records and electronic signatures, where practicable.

GPEA's caveat – that agencies need only implement e-business "where practicable" – was reinforced by the official GPEA guidance issued by the Office of Management and Budget (OMB) on May 2, 2000, 65 Federal Register 25508 (May 2, 2000) (available at the Federal CIO Council's home page, http://www.cio.gov). Under the OMB guidance, agency plans to implement e-business were to be submitted by October 2000, with electronic records and signatures, per GPEA, to be implemented by October 2003.

GPEA focused upon agencies' own gradual implementation of e-business. In the commercial sector, however, two important pieces of legislation have allowed e-business an abrupt advance.

The first piece of legislation is a uniform state law, the Uniform Electronic Transactions Act (UETA), which almost half of the states have adopted. Because UETA is relatively uncontroversial, eventually all the states are expected to adopt it. UETA gives electronic business critical legal legitimacy: under UETA, electronic signatures can be used to create enforceable contracts, and those contracts can be stored and presented in electronic form.

The progress of UETA in turn spurred Congress to pass the Electronic Signatures in Global and National Commerce (ESIGN) Act, Public Law No. 106-229 (June 30, 2000) (passed as S. 761) (to be codified at 15 USC 7001 et seq.). The ESIGN Act adopted the core principles of UETA: the federal act, like the uniform state law, provides

The OMB guidance points out that the ESIGN Act allows, but does not require, federal agencies to adopt electronic contracting methods. The OMB guidance notes that Section 104(b)(4) of the ESIGN Act allows agencies to specify particular authentication technologies in procurement. Finally, the OMB guidance emphasizes that GPEA – for which, as noted, OMB also had issued guidance – *requires* agencies to implement electronic signatures and records by October 2003, where practicable.

The Federal Acquisition Regulation (FAR) also is being amended to accommodate e-signatures. The pending FAR amendment, 65 Federal Register 65697(available at http://www.contracts.ogc.doc.gov/cld/facs/farcase2000-304.html), notes that, per GPEA, by October 2003 agencies must allow e-transactions where practicable. The FAR amendment, by emphasizing that electronic signatures can be accepted by agencies, is intended to ease the agencies' use of e-signatures and e-records in procurement.

Department of Defense PKI Implementation

The legal progress under UETA and the ESIGN Act, and GPEA's requirement that agencies implement e-business, have served as a backdrop to DoD's implementation of e-business using PKI. Key planning documents in the DoD initiative have included:

- The DoD Chief Information Officer (CIO) issued an important memorandum outlining the DoD's plans to implement PKI, "DoD Public Key Infrastructure" (12 Aug 2000) (http://www.c3i.osd.mil/org/sio/ia/pki).

- DoD has also issued a draft policy, "Public Key Enabling of Applications, Web Servers & Networks." This draft policy has raised some concern because it suggests that DoD intends to migrate to a "Class 4" assurance level for all PKI. That assurance level – and the security requirements it would impose – generally exceed commercial requirements for PKI. That concern is compounded because the draft policy would establish a procurement preference for PKI applications that could interoperate with the DoD PKI. If this meant that only those applications that could

- DoD x. 509 Certificate Policy Modified for Interim External Certificate Authorities (IECA) (May 4, 1999) (http://www.disa.mil/infosec/pkieca/documents.html): This document sets requirements for non-DoD certification authorities that are to interoperate with the DoD PKI system.

- DoD Class 3 PKI Public Key-Enabled Application Requirements, v. 1.0 (13 July 2000): This document sets forth proposed requirements for DoD applications that are to be PKI-enabled. DoD organizations are to use the document as the minimum requirements to select commercial products that are PKI-enabled, or include the document's requirements in establishing the overall requirements for development and acquisition efforts involving PKI-enabled applications. Government organizations also are to use the document's requirements as a basis for testing applications' ability to interoperate with the DoD PKI.

- DoD Class 3 Public Key Infrastructure Interface Specification, v. 1.2 (10 Aug 2000): This specification describes the interfaces to the DoD Class 3 PKI needed by users and application developers. The specification is intended to facilitate a common infrastructure instead of multiple, potentially overlapping or redundant systems, as well as compatibility with the DoD PKI, other parts of the Federal Government, and the commercial world. The specification also states that DoD is committed to the use of commercial standards and to evolving as those commercial standards evolve.

- X.509 Certificate Policy for the United States Department of Defense, v. 5.1 (21 Sept. 2000): This document is the unified policy under which Certification Authorities operated by DoD components are established and operate. It includes policy for the creation and management of Version 3 x.509 public-key certificates for use in applications requiring communications, including electronic mail, transmission of unclassified and classified information, signature of electronic forms, contract formation signatures, and authentication of infrastructure components. It does not define certificate policy for Certification Authorities operated by external entities on behalf of DoD; that separate policy is discussed above. The policy provides that a non-US government subscriber will have no claim against DoD arising from use of the subscriber's certificate or termination of that certificate. In addition, DoD will not

- X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA), v. 1.06 (23 Oct. 2000): This document defines the certificate policy for use by the FBCA to facilitate Agency Certification Authorities' interoperability with the FBCA and with other agency PKI domains. The v. 1.06 policy does not provide for interoperability through the FBCA between federal agency PKI domains and those parties external to the federal government who have no regulatory or contractual relationship with the federal government. The document provides that agencies desiring to interoperate using the FBCA must seek approval through an application process and enter into a memorandum of agreement which sets forth the respective responsibilities and obligations of the parties. The policy disclaims any US government liability that may arise from use of any certificate issued by the FBCA, including direct or indirect, incidental, consequential, special, or punitive damages. In addition, the policy provides that the government retains exclusive intellectual property rights to any products or information developed under or pursuant to the FBCA Policy.

Emerging Legal Issues in DoD PKI

The DoD's planning documents for PKI have raised a number of legal issues. These issues, reviewed below, stem mainly from expansive preliminary positions in the planning documents. Early discussions indicate that these issues may be resolved, as the PKI planning process evolves.

1. Liability Issues

The first area involves potential liability, should there be failures in the PKI system. This is clearly a key emerging issue, for the DoD planning documents – including the DoD Public Key-Enabled Application Requirements, at section 3.2.2 -- anticipate high-value financial transactions.

To date, the guiding documents indicate that DoD (and other agencies) may seek sweeping exemptions from liability. For example, the DOD x.509 Certificate Policy § 2.2.1, v.5.1 (21 Sept. 2000), disavows all DoD liability for

These disavowals of liability raise a host of issues. Simply forcing all liability on to private parties may be an inefficient allocation of liability – and thus may raise new contracting costs. This approach also may narrow the field of prospective vendors, for generally only larger, more sophisticated vendors can self-insure or "outsource" risks displaced to the private sector, as the result of the government's attempts to disavow any liability.

Key planning officials have suggested that industry concerns about liability may be overdrawn, either because the actual prospective liability is relatively small or because the government has not, in fact, disclaimed liability as broadly as the planning documents have suggested. This is an area that would benefit from further free and frank discussions between industry and government; otherwise, the liability issues may raise barriers to the government's implementation of PKI.

We would recommend that DoD look to evolving commercial norms and guidance for allocating liability. Commercial certification authorities, for example, typically do not disclaim all liability, but instead generally limit liability through their Certificate Practice Statements (CPS). See, e.g., Verisign Certification Practice Statement v. 1.2, section 11.6 (May 1997) (available through http://www.verisign.com/cps). The American Bar Association, Science & Technology Section, Information Security Committee (ISC), had published Digital Signature Guidelines (http://www.abanet.org/scitech/ec/isc/dsgfree.html), which discuss the allocation of responsibility in a PKI architecture. The ISC is currently developing Public Key Infrastructure Assessment Guidelines (PAG), see http://www.abanet.org/scitech/ec/isc/home.html, which will allow users – public and private – to guide assessments of PKIs. The PAG, currently in draft form, offers a detailed analysis of lines of responsibility and liability through a PKI architecture.

TPAs have long been part of e-business in the commercial world. See, e.g., Uniform Electronic Transactions Act, sec. 1, reporter's comment 1 (citing Model Trading Partner Agreement, 45 Business Lawyer Supp. Issue (June 1990)). DoD units have themselves begun using TPAs to allocate risks in contracts that require electronic transactions. See, e.g., Military Traffic Management Command, EDI Trading Partner Agreement for Defense Transportation, at 9 (Jan. 1998) (model TPA) (available at http://dcsop.memc.army.mil/freight/trading/tpa.html).

2. Intellectual Property Issues

The PKI planning documents also suggest that the government will take an expansive approach to intellectual property rights. The core DoD planning document, the DOD x.509 Certificate Policy, at section 2.7, states for example that the DoD "shall maintain ownership of any public key certificates and private keys that it issues." And the Federal Bridge x.509 Certificate Policy § 2.7 says that the Government "retains exclusive rights to any products or information developed under or pursuant to this" certificate policy.

Sweeping government assertions of intellectual property rights may restrain commercial adoption of PKI. More immediately, if the government asserts sweeping intellectual property rights, commercial vendors may refuse to develop or provide PKI solutions for the government marketplace. Per the DoD's draft policy, "*Intellectual Property: Navigating Through Commercial Waters*," we would recommend that government agencies take a more flexible approach to intellectual property issues to ensure agencies' access to commercial information technology solutions.

3. Procurement Issues

Competing vendors may protest that DoD is unduly restricting competition -- and thus is violating the Competition in Contracting Act -- by planning to migrate to Class 4 security procedures for all PKI, and by forcing vendors to absorb or "out-source" risk to

Although the FACNET system was flawed from the start, and competitive vendors were sometimes hobbled by those flaws, the General Accounting Office (GAO) proved reluctant to hold that the Competition in Contracting Act (CICA) requires the government to fix FACNET to level the competitive field.

As a backdrop to FACNET, the GAO's decisions said that the government could set minimum technology requirements for its vendors, if those vendors were to exchange information electronically with the government in competing for federal contracts.

In Arcy Manufacturing Company, Comp. Gen. No. B-261538, 1995 WL 479664 (Aug. 14, 1995) (unpublished), several small businesses challenged the requirement of the Defense Industrial Supply Center (DISC) (of the Defense Logistics Agency) that firms respond to certain requests for quotations (RFQ) by electronic transmission. The protesters argued that this requirement overly restricted competition, in violation of the Competition in Contracting Act. The RFQs at issue were published through a DISC electronic bulletin board, which could be accessed only by computer. The protesters argued that this system in effect precluded them -- and thus unreasonably restricted competition -- because the protesters did not own computers.

The agency's arguments in response probably echo at least some of the arguments the DoD will make here, if vendors object to being forced into a PKI system. The agency in Arcy Manufacturing argued that its computer-based system had substantially reduced its costs of contracting. The agency pointed out that, "in contrast to the paper system which required manual receipt, processing, recording, and filing of the paper quotes, electronic quotes are automatically received, recorded, and distributed to the cognizant DISC buyer through DISC's computer system." The agency reported that its electronic method allowed DISC to reduce its time to complete small purchases from 100 days to 20 days, and that the labor hours per purchase were reduced from 7 hours to 3 hours. Id. at 2.

The agency also argued that the electronic procedures in effect broadened competition. The agency noted that, through the use of its electronic bulletin board, it

The GAO accepted the agency's arguments as a reasonable basis for requiring vendors to respond through an electronic bulletin board. Citing an earlier Comptroller General decision that had held it was not unreasonable to require vendors to use a personal computer, id. at 3 (citing Essex Electro Engineers, Inc., Comp. Gen. No. B-252288.2, 93-2 CPD ¶ 47 (July 23, 1993)); the GAO held that "the agency has a reasonable basis for requiring that quotes be submitted electronically and that this requirement is not overly burdensome on the vendor community." Id.; see also Commonwealth Industrial Specialties, Inc., Comp. Gen. No. B-277833 (1997) (vendors reasonably be required to use an electronic bulletin board for procurement, so long as not unduly burdensome).

The Arcy Manufacturing decision thus cleared the way for agencies to require vendors to adopt common technology for electronic procurement, so long as that technology was not "overly burdensome." What was left unresolved, however, was how GAO would deal with failures in that technology, when the government adopted FACNET, a much more broadly based electronic procurement system.

Initially the GAO took a stern stand on FACNET. In the first GAO decision under FACNET, S.D.M. Supply Inc., No. B-271492 (June 26, 1996), reconsid, 96-2 Comp. Gen. ¶ 203 (Nov. 27, 1996), the GAO held that where an agency had allowed systemic failures in the FACNET system, and a contractor's bid was lost as a result, under CICA the government would have to reimburse the contractor its bid-and-proposal costs. In that case, the agency had lost the protestor's electronic bid, which had been submitted through the FACNET system. The GAO held that because the agency had not made "reasonable efforts" to safeguard electronic quotations, the agency was liable to the contractor.

On its face, S.D.M. Supply would seem to suggest that if agencies erect a PKI architecture to protect the procurement process, and agencies do not make "reasonable efforts" to ensure that transactions within that PKI architecture are secure, under CICA agencies may be liable to contractors if bidding processes fail. Subsequent decisions from GAO, however, narrowed the force of S.D.M. Supply.

The decision in American Material suggests that, if failures in the PKI system impact procurements at contract inception, bidders will not be able to recover unless the failures are due to "systemic" (or even purposeful) omissions by an agency. This means, in turn, that agencies would be well served to plan and build their PKI architectures carefully. Careful planning and construction should help to reduce "systemic" failures; then, if episodic, non-"systemic" PKI failures occur in the bidding process, agencies will be less likely to face liability under CICA.

The cases discussed above involve failures in the bidding process, caused by failures in the FACNET system. Another case inspired by FACNET addressed a different problem that is likely to arise as PKI is implemented: unfairly onerous requirements, which shift too much risk to contractors.

In Simplix, Comp. Gen. No. B-274388, 96-2 Comp. Gen ¶ 216 (1996), a VAN that wanted to participate in FACNET protested to the GAO that the government, by changing requirements for the private VANs, was imposing too much risk on the private network providers that completed the FACNET system. The GAO rejected that argument:

> Many of Simplix's other complaints focus on what Simplix believes is an unfair allocation of risks between the government and the EDI VAN provider . . . . Simply stated, Simplix asserts that the EDI VAN provider is expected to assume the bulk of the responsibilities and risks. Simplix complains in this regard that VANs already carry all costs associated with failures of the electronic commerce infrastructure, including accounting for lost transactions, and face the burden of marketing the government's EDI system, yet the government makes no adequate guarantees regarding its technical obligations in operating the EDI system. *Risks are inherent in procurements and the government may properly impose substantial risks on firms contracting with the government and minimal risks upon*

Id. (emphasis added). The decision in Simplix suggests that, if the government erects a PKI architecture that shifts serious costs and/or risks to contractors, bidders will have do show that the government's approach "unduly inhibits" prospective contractors.

The cases spawned by FACNET lay the following groundwork for bid protest challenges to a PKI system, if it is mandated by DoD or other government agencies:

- Vendors will have difficulty prevailing on an argument that *no* PKI requirements should be imposed, because PKI security is regularly used in the commercial marketplace.

- If there are failures in the PKI architecture that cause bids to go astray, or otherwise cripple the contracting process, bidders will likely have to show that those failures are "systemic" in order to prevail.

- If agencies continue to shift PKI risks to the private sector, protesting contractors will have to show that the government's efforts to shift risks "unduly inhibit" prospective contractors.

We should emphasize that the decisions discussed above involve only *bid protests*, which stem from failures in *contract formation*. Even if vendors cannot prevail on formal bid protests, vendors effectively excluded by DoD security requirements are likely to carry their arguments to Congress, the Small Business Administration (SBA), and the White House. And if failures in the PKI system create costs during *contract administration*, those additional costs will result in *claims and disputes*. Because PKI is still an emerging technology, neither the boards of contract appeals nor the Court of Federal Claims have addressed how liability should be allocated for PKI failures during contract administration; in practice, the allocation of liability is likely to turn on the language of the governing contracts.

Technical Issues in PKI

Work Group Participants

Patrick Arnold, Co-Chair, Microsoft
Gary Moore, Co-Chair, Entrust Technologies, Inc
Charlie Booth, Cisco Systems
Chris Dobbs, Spyrus
Rachel Shea, Baltimore Technologies
Robert Thomson, RSA Security

Introduction

The DOD ASD C3I August 12 Policy Memo calls for DOD to evolve to Class 4 certificates for all environments and applications that employ public key technology. Migration for certain mission-critical components must be completed by December 31, 2003; for all other environments by December 31, 2006. While the Memo describes the strategy as one of enabling security services at multiple levels of assurance, ultimately all the focus of the document is upon the Target Class 4 environment for all components.

The Deputy CIO and the Director of Defense Reform have asked for an impact statement from industry. This FECC working paper is intended to provide industry recommendations in regards to the technical aspects of the implementation of this policy as that relates to the impact on the Department's ability to utilize the DOD PKI to transact business with agencies and organizations outside of the field of operations. This paper will also highlight trends within industry implementations and planning which the Department may take advantage of in its implementation strategy. The output of this paper will be a set of recommendations which the industry partners believe will allow the DOD PKI to provide a set of services which place minimal requirements on the end user (that is, the security functions and trust decisions are not intrusive) and will provide a development environment in which the functional groups can efficiently and effectively integrate security services into their programs in such a manner as not to be dependent on a single source of security services.

Background

The Department of Defense has currently implemented or is in the process of implementing an internal KMI strategy which encompasses a number of key initiatives including the Defense Messaging System (DMS), the Class 3 Medium Assurance PKI, the emerging Class 4 PKI and the Interim Certification Authorities. The development of the associated infrastructures and the relationships between the individual technology elements within a specific program has been well defined and consistent for internal DOD use. Recently DOD has refined its application requirements to extend beyond the services originally described in the August 1998 specifications. These initiatives are very key for the development of the internal strategy. Concurrent with DOD's development and implementation process a number of initiatives, within the commercial sector and within the Civilian Agencies of the US Federal Government and other governments, have lead to rapid development of a number of architectural concepts and processes which will greatly assist the Department in its ability to deal with its business partners utilizing an e-business strategy.

Three areas of focus will be taken in this paper: Trust Interoperability, Directory Interoperability and Application Integration. The key goal in the consideration of these elements is to ensure that the business processes which utilize the developing PKI will demand consistency, ease of use, scalability, transparency and security. These features will also be demanded of the developers of the applications which will implement these processes. The next three sections of the paper will address each of the three focus areas individually.

Trust Interoperability

The development of the internal KMI strategy which encompasses a number of key initiatives within the Department has seen the implementation of three PKI Programs specific to the Department; the Class 3 PKI, the DMS PKI and the IECAs. Continuing evolution will see the near term implementation of the Class 4 PKI, which in most aspects will be an evolution of the Class 3 since it is based upon the evolving requirements defined around the Class 3 PKI. As a result of these ongoing initiatives the Department has effectively implemented or will implement three separate PKI methodologies/systems. These include the DMS PKI, the Class 3 PKI with its evolution

It has also been stated that DOD will interact with the Federal Bridge Certification Authority (FBCA) (reference Department of Defense Class 3 Public Key Infrastructure Interface Specification, Version 1.2, 10 August 2000). Additionally it is wholly conceivable that the Department will have need to interact with vendor specific PKIs, such as those run by DOD suppliers, healthcare providers, or other business partners, and/or with users which have obtained certificates through GSA's Access Certificates for Electronic Services (ACES) Program.

Each of these systems, although based upon the general X.509 construct, have specific architectural and functional elements that make the concept of consistent user interaction based upon a consistently implemented business process difficult. An example of this would lie in the verification of a signature on a document which was created by a vendor using a Business ACES certificate and then sent to a user of the Class 3 PKI. For the internal DOD user to verify this document he must be able to construct a trust path to the ACES CA. In the ACES model this is achieved through an interaction with the Certificate Arbitrator Module (CAM). In the future this interaction will be via OCSP. The interaction would inform the user if the certificate is that of a valid and current user. The application and/or the user would then need to determine if the policies associated with that CA meet the specific application requirements.

The interaction for the user's application would be somewhat different if the external party was a user of an IECA CA. In this scenario the application would make its status decision of the user through the processing of the certificate and the validation of the status of the user through a CRL verification check since both end entities would have the appropriate trust root installed in their trust list. Once again the user and/or application would need to make the policy evaluation.

The third scenario may occur when DOD implements use of the Federal Bridge. In this scenario the trust decision will be based upon an evaluation of the trust path that is developed utilizing the X.509 state engine. This evaluation would include status checking of various certificates in the path utilizing standards based mechanisms; today these are likely to be CRLs but in the future they may include other mechanisms such as OCSP or other such developing protocols. Once again the policy evaluation will need to be assessed by the application and/or end entity.

The mechanisms do place differing requirements on the applications and the parties involved. The ACES example and similar structures require the use of OCSP and a strong implementation in the infrastructure of the policy rules and constraints. This mechanism may also require specific knowledge of how to communicate with the servers within the infrastructure. In today's implementations, such as ACES, the relying party needs to be able to communicate with specific servers in the infrastructure where the trust decisions are made. Ongoing work, such as that within the Identrus environment, has influenced PKI vendors to ensure that their products can support the specific policy implementations and certificate profiles required in that environment.

Implementations such as those like the IECA require that the relying party and the end entity have their trust rooted by the same authority. This model works well within the Department but imposes difficulties to the outside communities, due to the requirement to have their trust infrastructures certified under the Departments.

The Bridge model also faces challenges. Today the common understanding of the bridge architecture relies strongly on interoperable directories and the ability for applications to traverse these directories in a consistent way to develop the trust paths. Directory Interoperability will be discussed in the next section. The common application requirements to work in this environment are also evolving based upon ongoing work within the Federal Bridge CA effort and the DOD Bridge CA Demonstration. The output of both of these initiatives has driven application, directory and CA vendors to work more closely in the realm of interoperability and path processing.

Directory Interoperability

The ongoing efforts within the Department, as they relate to PKI, have been strongly influenced by and in turn have strongly influenced the development of an agency wide directory. The current PKI implementations within the Department rely on the ability to utilize the common directory structure as a repository for certificate information and certificate status information, today in the form of CRLs.

Industry has driven some fundamental changes with respect to reliance on the directory as the sole source of information on which to base trust decisions. The current model is effective but faces some very significant challenges. Large Scale Implementations of

These mechanisms provide direct reference to the elements on which the trust decision can be built. This is an area of current work and one worthy of watching. A second alternative is to rely on a Certificate Validation Model to perform the trust evaluation. This could potentially reduce the requirement for interoperable directories since it would be built around the concept that the validation server would have access directly to the appropriate repositories. Again this is an area of ongoing work with the ongoing development of the appropriate protocols such as OCSP, OCSP-X, SCVP and others.

The trust path development problem, and its potential requirement for interoperable directories, becomes exacerbated when encryption capabilities are needed across those same domains. A trust path development requires that a path be developed between two ends of trust. To discover an end entity's public encryption certificate requires that the system be capable of searching the entire directory structure based upon some simple search criterion such as Common Name.

Application Integration

The effect on the end user of issues raised in the last two sections becomes apparent through the application that they use. The goal of the application environment must be simplicity for the end user. For an appropriate trust decision to be made, one of two things must happen: (1) Either the application must present to the relying party all the appropriate information that has been discovered when evaluating the trust path, such as end entity information, end entity status, CA information and status and policy information, leaving the end user to make the trust decision; or (2) the application must evaluate these elements based upon the defined policy within the department and within the specific business process, and report whether the transaction can be trusted.

In either case, this evaluation by the application can be looked at in two distinct phases: Path or Certificate Validation and Policy Evaluation. Path or Certificate Evaluation can be achieved through the mechanisms we described in the Trust Interoperability section. Once we know that the presented certificate passes the basic criteria (that it has not been tampered with, is within its valid date range, has not been revoked and is from a party we trust at some level), then the relying party must be able to evaluate the ability to use the specific certificate based upon policy. Policy may require that the CA meet certain

These constraints need to be evaluated based upon the information gathered either during or after the path validation. There has been considerable progress made in regards to path and certificate validation. Today industry has seen some use of OCSP within COTS applications for certificate status checking. Other products are capable of evaluating certificates utilizing the mechanisms of URL as per RFC 2459. More products have implemented full X.509 path discovery and validation and recently freeware toolkits have become available to implement these mechanisms in products. Industry has seen only a few implementations of automated policy and constraint processing but this is an area of work within the current DOD Bridge CA Demonstration effort. This will be an area of further growth in the near to medium term.

Conclusions

It is the opinion of the FECC PKI Technical Sub Group that industry, working with the Federal Government and the commercial sector, has worked to implement a broad array of solution alternatives to aid in the implementation of e-business initiatives. Within the areas discussed - Trust Interoperability; Directory Interoperability and Application Integration - solution sets are available to deliver the services needed. Within the Department of Defense some of these solutions sets would interoperate with the existing environment without greatly affecting direction but would require additional research to determine best practice. Given the areas covered the Technical Group would like to make the following recommendations:

- Following the existing direction of interoperation with the Federal Bridge CA is a viable alternative to achieve interoperability with other Federal Agencies. In this regard the Department should continue its initiative as a funding partner.
- Implementation of a DOD Bridge would allow closer control of policy and interaction with business partners.
- Encourage the other trust architectures to interoperate with either the Federal Bridge or a DOD Bridge.
- Following the existing plan to implement OCSP as an alternative trust architecture or one that complements the existing architecture is prudent.
- Commit resources to the further investigation of directory influences. This should include direction towards interoperability of existing and planned directory architectures as well as investigation of alternatives such as RFC 2459 processing to

- Provide to the business process developers a more concrete solution set for application integration. The current Application Interface specifications are open enough to result in application developers spending a large amount of time and resources in developing capabilities that today can be achieved with the integration of COTS and freeware toolkits. The Department should encourage the application developers to utilize these existing tools.
- Further development in the application area is happening at a rapid pace within the XML community. The Department should follow this closely and become involved in demonstrations efforts at the earliest possible times.
- The industry partners bring a considerable level of expertise to this effort. The Department should continue to support such initiatives as the FECC.

Policy Issues for External eBusiness using PKI

Work Group Participants

Rusty Wall, CSC, Chair
Katherine Hollis, EDS
Bob Daniels, EDS
Gene Hilborn, CSC
Tom Greco, Digital Signature Trust, Co
Rachel Shea, Baltimore Technologies, INC
Joe Mirabile, OSD (provided information on DoD PKI Policies)
Rebecca Kahn, Federal PKI Steering Committee, (advisor on Federal Bridge CA)

Background

Per the DoD PKI policy memo, the milestone to migrate to Class 4 by Dec 2003 is for Mission Critical systems operating on unclassified networks only. All other systems in all other operating environments may continue to issue Class 3 certs until Dec 2004. With three-year expiration, systems may theoretically operate until end of 2007 using Class 3. Although the draft PKE policy memo indicates 2006 to get Class 4 enabled, that's from the perspective of the system/application owner, so that they would have the capability to turn on this feature no later than end of 2007.

While the Memo describes the strategy as one of enabling security services at multiple levels of assurance, ultimately all the focus of the document is upon the Target Class 4 environment for all internal DoD Components.

The Deputy CIO and the Director of Defense Reform have asked for policy-related comments concerning their current program and its impacts on potential external (to the DoD) e-Business.

As a result, this FECC working paper is intended to provide background on DoD Policy-

Problem

DoD is a Federal Department that operates in a world of emerging e-Business and e-Government practices. Acknowledging this reality, DoD has an aggressive program to implement a PKI-based Global Information Grid to address its internal security requirements.

It is our view that DoD needs a comprehensive and coherent policy and strategy addressing the use of PKI for e-Business with non-DoD entities. **Specifically, DOD needs implementation policy concerning the acceptance by DOD components of PKI certificates other than DoD's own Class 3 and future Class 4 system. We believe this is a potentially critical need which, if not addressed, could result in DoD's inability to leverage rapidly developing commercial PKI-enabled e-commerce systems.** While nothing in the current DoD policies explicitly prohibits DoD applications and users as relying parties from accepting and relying on certificates issued by non-DOD parties, including certificates below the DoD Class 4 level of assurance, it is our view that the existing policy does not clearly delineate the flexibility which DOD components either should or may enjoy in making decisions as to which certificates are acceptable for their applications.

In its basic form, in a simple application, this problem is best exemplified as asking the questions, "What should the DoD do with the root certificates that are contained in the Netscape and Microsoft browsers other than the DoD trusted Class 3 root contained in there now?" "How should we develop a plan to determine and manage which of them are to be trusted for what purpose?" "What other trust roots may be added and used for what purpose?" "For the thousands of other DoD applications that are going to be PKI enabled, how is DoD going to set up trust paths to use the certificates issued to people and applications outside the DoD?" Yes, the DoD class 4 Certificate will be used inside DoD, but, "What other trusted roots will be also used and what are the trust paths to these other roots?" "What are the requirements, what trust levels are required; -what are the trust requirements of the owners of the applications, the relying parties?"

Without a policy that includes sufficient flexibility, the following unintended

- Reduced trading partner participation,
- Creation of an excessive and difficult infrastructure to manage and maintain,
- Inhibition of system interoperability,
- Excessive implementation costs, and, possibly,
- Diminished overall protection of sensitive information.

While it is acknowledged that industry is moving slowly to higher assurance levels similar to those mandated by the current DoD program, there currently is a gap between the high assurance DoD PKI program and the current trust levels in use or envisioned in the near term in commercial industry and in other Federal agencies.

Different applications require different certificate levels of assurance; the higher the assurance level, the higher the cost of implementation. We respect DOD's determination that the highest achievable level of assurance with current or envisioned PKI technology is required for core DoD functions and for ensuring the integrity of DoD networks. However, the August 12 memo could be interpreted to require the highest level of assurance for all DoD support functions and for all of DoD's business partners (i.e., industry). It is questionable whether this level of assurance is currently achieved by or is economically acceptable to industry (and other parts of Government). Moreover, it is unclear whether the highest levels of assurance are justified or necessary for most business functions requiring interaction with DoD elements.

By requiring such a high level of assurance, DoD would be imposing excessive infrastructure costs on itself and its business partners. This is likely to slow adoption, reduce participation, and possibly even diminish security as DoD partners may choose not to use the PKI, or use a PKI that DoD does not recognize.

The commercial sector is undergoing its own evolutionary process in the use of PKI. This process is taking different paths in different commercial domains, with a "domain" defined as encompassing areas like B2B (EC/EB), healthcare, personnel/retirement, financial services, and logistics. It appears that security models employing authentication based on certificates having lower levels of assurance than Class 4 are experiencing widespread use. The drivers for security and privacy are different for each domain and are different from DoD's fundamental drivers for Information Assurance.

Rather than appearing to require that DOD security procedures and infrastructure be employed in these domains, DoD may be better served by:

- individually evaluating its security and trust requirements for activities in these domains,
- working in partnership with its external trading partners to reevaluate the joint trust and security requirements for each domain, and
- where appropriate, accommodating its external business processes in certain functional areas to the emerging commercial standards for those domains.

This paper does not attempt to address what the appropriate policies should be for specific DoD activities. Our goal is to highlight the approaches that should be examined and to urge the DoD to develop a strategy for adding trust through alternative PKI approaches by communicating with representatives from the emerging activities in the private and non DoD Federal sector.

New Opportunities

One challenge facing DoD, or any PKI-enabled enterprise that touches multiple commercial domains, is how to interpret and accept certificates issued by other organizations and under different policies. Because this is very difficult, the default response has been to choose not to accept certificates issued by other entities at all.

However, **two developments** have made the prospect of interoperating with other PKI's more likely both on a policy and on a technical level:

- **The development of the Federal Bridge CA** offers a *convenient* mechanism for DoD to accept certificates originating outside DoD, at various Class levels.
- **The emergence of broad community-of-interest (COI) PKI's** (i.e., a PKI serving a large community of separate enterprises for e-commerce, or e-Government purposes) in the commercial and Federal sectors similarly offers a simplified mechanism for the DoD PKI to accept certificates from major domains with which it does business.

Preliminary Recommendations:

- **The DoD should develop a strategy and associated policies for PKI implementation that includes a roadmap for trust relationships and the development of relying party trust requirements in communications external to DoD using PKI.**

  - This strategy and associated policy should consider the use of the Federal Bridge CA for interoperating the DoD PKI with non-DOD Federal agency PKIs, and even PKIs external to the Federal government.
  - The DoD should consider other policy and technology approaches for evaluating and accepting certificates issued in non-Federal PKI Communities of Interest ("COIs") such as alternative bridge or cross certification arrangements that provide for accepting less-than DoD Class 4 assurance
  - The strategy and associated policy should define complete, yet sufficiently flexible requirements for use/acceptance of non-DoD PKI certificates for dealing with parties external to DoD.
  - The strategy and associated policy should specifically not preclude the acceptance and reliance on Class 2 and 3 equivalent PKI certificates where their use in an external e-Business environment is appropriate.

- **The DoD should also develop a strategy and plan to assess its external business processes to determine its internal relying party trust requirements for the proper combination of technology and management controls to manage the risk of converting transactions and record keeping to electronic form, and then conducting transactions electronically.**

  - Each assessment should contain elements of risk analysis and measurements of other costs and benefits to determine the trust requirements required for the particular transaction type. This means non PKI-based electronic transaction authentication mechanisms, DoD class 2, 3 and 4-equivalent methodologies and additional trust requirements within the current PKI classification structure required for the application type.
  - The strategy and plan should encourage functional element COIs (including both

- **The DoD should examine its current and draft e-Business policies and ensure that the use of non-DoD PKI alternatives is addressed appropriately, considering both pros and cons. This means to both encourage and discourage their use as appropriate.**

    - Functional communities should explicitly identify their assurance requirements in their associated e-Business policies.
    - The appropriate e-Business policy should be updated or appended to include such requirements.
    - As an example of an e-Business –related policy under development by OSD, the November 2, 2000 Draft ASD (C3I) Memorandum on Public Key Enabling of Applications, Web Servers and Networks for the DoD should be modified to incorporate an examination of the relying party assurance levels required for applications within DoD for external and non class 4 DoD certificates. Perhaps the Draft PKE policy could add a sentence in the paragraph that calls for business case analyses to ensure that relying party assurance requirements are included in that analysis. Additionally, this process should be defined and explained in the policy. Furthermore, this draft policy memorandum could be an appropriate place to expand upon:

- the plans for use of non-DoD Class 2 and 3 certificates addressed in brief in the current DoD X.509CP in paragraph 1.3.4.6,
- the necessity to set up relying party policy for non-DoD certificates partially addressed in DoD X.509CP paragraph 2.1.4 and,
- the procedures and roadmap for the PMA to move forward to authorize the use of non-DoD certificates addressed in brief in the current DoD X.509CP in paragraph 8.3. (These issues are highlighted further in the attachment following this section.)

Follow-on recommendations:

- The FECC PKI working group should further examine the topic and postulate external business partner policies wherein DOD would accept different levels of assurance for outside DOD transactions based on the working group's conclusions and recommendations.
- The FECC PKI working group should further provide recommendations concerning

Attachment to Policy Section

Potential added value to DoD for encouraging the use of externally issued non-DoD Class 2 and Class 3 certificates in certain appropriate cases

---

Added Value to DoD may include the following uses:

CLASS 2 CERTIFICATES (equivalent to FBCA Basic Level of Assurance)

Types of External Business Applications

- Intra-or Inter-organizational email external to DoD
- Web intranets or extranets, small, "low-risk" transactions
- Personal/individual e-mail
- Password replacement and software validation.

Business Value

- Primarily for administrative functions that require a higher level of identify proofing to support processing low-risk administrative services such as: travel, payroll, and small and medium value financial transactions (office supplies, subscriptions, vehicle inventory, payroll).
- Identity proofing is accomplished by verification of an existing e-mail account and the existence of the identity by established commercial databases such as credit reporting firms, and/or assertions by responsible company personnel (e.g. checking against the HR directory).
- Class 2 Certificates may also be issued to network devices to provide a more manageable and trusted network environment (e.g. in support of DEN).

CLASS 3 CERTIFICATES (equivalent to FBCA Medium Level of Assurance)

Types of External Business Applications

- In addition to Class 2 uses, uses are e-banking, database access, transport and access of privacy sensitive information and email (e.g., health records, business plans), e-commerce server, software and validation, and high volume/moderate value business transactions.

Business Value

- Provides a high assurance of confidentiality, information integrity, authentication and non-repudiation to a broad array of business transactions and exchanges.

Although the current DoD X.509 CP partially addresses some aspects of the use of non-DoD certificates, recommend that the DoD consider addressing the issues specifically addressed in the paragraphs below in the new November 2, 2000 Draft ASD (C3I) Memorandum on Public Key Enabling of Applications, Web Servers and Networks for the DoD.

These issues are as contained in the current DoD X.509CP sections:

- **1.3.4.6 Use of non-DOD certificates**
- **2.1.4 Necessity to set up relying party policy for non-DoD certificates**
- **8.3 CPS and External Policy Approval Procedures**

This draft Memorandum would be a more appropriate place to address the use of non-DOD certificates than the DoD X.509 CP that has, as its primary purpose, addressing the issuance, management and use of DoD's own certificates.

For ease of reference, the following paragraphs are extracted from the DoD X.509 CP.

These extracts are intended to not only illustrate current DoD policy but also to illustrate the need to encourage the use of Class 2 and Class 3 certificates from sources outside DOD for use in e-Business or other electronic transactions with non-DoD elements. (highlighting has been added for ease of reference)

- ***1.3.4.6 General usage***

DOD Class 2: *This level is intended for applications handling unclassified information of low value in a Minimally or Moderately Protected Environment. DOD CAs will not issue CLASS 2 certificates; the DOD shall issue CLASS 3 and CLASS 4 certificates exclusively. Access to DOD information resources shall never be allowed on the basis of CLASS 2 certificates.* ***CLASS 2 certificates, (or non-DOD equivalent certificates) may be accepted by DOD relying parties for the purpose of authenticating or encrypting communication that does not access or process DOD information (meeting coordination, accessing web site information that has been cleared for unlimited distribution. etc.) These certificates may, for example, be issued by non-DOD commercial entities, and be used to authenticate communications with external vendors.***

DOD Class 3: *This level is intended for applications handling unclassified medium value information in Moderately Protected Environments, unclassified high value information in Highly Protected Environments, and discretionary access control of classified information in Highly Protected Environments.*

Guidance:

- *All applications appropriate for CLASS 2 certificates;*
- *Digital signature services for mission critical and national security information on an encrypted network;*
- *Privacy and authentication in support of access control security services (e.g., separation of communities of interests) for access to classified Special Compartmented or Special Access information on networks protected using NSA approved Type 1 cryptography appropriate to the data being protected, or on networks that are physically isolated and approved to process the classified data.*
- *Technical non-repudiation for small and medium value financial transactions other than transactions involving issuance or acceptance of contracts and contract modifications. This would include acceptance and payment for small and medium value financial transactions, travel claims, payroll, etc.*

***2.1.4 Relying party obligations*- (This section of the DoD X.509 CP was not extracted because it only addresses the use of DoD Certificates.)**

8.3 CPS and External Policy Approval Procedures

The PMA shall make the determination that a CPS complies with this policy for a given level of assurance. The CMA must have and meet all requirements of an approved CPS prior to commencing operations. In some cases the nature of the system function, the type of communications, or the operating environment may require the additional approval of an authorized agency.

The Policy Management Authority is authorized to make the determination that other (non-DOD) CPs offer appropriately equivalent levels of assurance to the DOD CPs.
The PKI may respond to such decisions by methods including but not limited to:

- *issuing cross-certificates to other PKIs asserting other policies;*

FECC Industry Working Group
On DoD PKI Policy

Final Assessment Report

SUMMARY and RECOMMENDATIONS

In summary, it is the opinion of the IWG that the current DoD PKI Policy is a network centric policy and has not taken into account the varying DoD functional and operational requirements; systems applications; processes or policies existent in the day-to-day business operations within the DoD. Likewise the policy does not address, or take into consideration, the burgeoning e-Business environment that DoD is developing with its industry-based partners. Much of this business does not require the high level of security currently prescribed in the DoD PKI Policy. Even though at the close of this assessment DoD staff assured the IWG that follow-on guidelines for functional applications were forthcoming, there were no indications those guidelines would necessarily deal with the issues raised in this assessment.

Consequently, for the near to intermediate future, the current DoD PKI policy is a "one size fits all" policy for all users both within DoD, and those outside, who must interact with or use DoD systems.

Thus, the IWG makes the following recommendations for DoD's consideration:

1. Adopt and make operational the Federal PKI Bridge as the initial solution for external e-Business transactions and processes.

2. Create Industry "Domain" Panels/Working Groups to work with DoD functional communities on appropriate "levels of PKI transactions".

6. Write an external e-Business PKI policy and widely communicate the policy with DoD functional process owners and their Industry counterparts.

7. Specify how small businesses will be required to become PKI compliant.

8. Allocate liability risk efficiently and address the issue of intellectual property flexibility.

9. Develop a mechanism to share the FBCA solutions with commercial entities, so they may include the solution, if they choose, in their infrastructure.

10. Develop a process for reviewing, testing and readily adopting new commercial solutions in the Information Assurance domain.

In conclusion the FECC IWG stands ready to continue its support of the on-going DoD efforts to make operational, an effective and interoperable PKI solution for e-Business. The FECC IWG is appreciative of the support it received from the various members of the DoD's CIO staff as well others from the PKI Program Office, DISA and JECPO. We hope that our efforts are useful in furthering the strong mutual bonds required to forge an effective and secure e-Business environment between the DoD, Federal government and Industry.

Attachment 1

DoD PKI Policy Impact Assessment
(21 September 2000)

Purpose: To provide an assessment on eBusiness of the impact of the August 12, 2000 ASD(C3I) Memorandum, Department of Defense (DoD) Public Key Infrastructure (PKI).

Background: Providing for secure and trusted commerce is one of the major barriers to successful forward movement of DoD and Federal electronic business. The August 12, 2000 PKI Policy update aligned the PKI and CAC Programs and reaffirmed the DoD PKI policy. Now that the final policy piece is in place, implementation actions must be planned and carefully executed. To assist in performing this planning and execution, it is advisable for DoD to have an independent impact assessment that will present both public and private sector impacts and considerations. The Federal Electronic Commerce Coalition (FECC), through its members, working in conjunction, has offered to provide a comprehensive impact assessment using the new PKI policy memorandum as well as such corollary documents as the GAO EB report and ECCWG security recommendations.

Guidelines: The assessment will address but not be limited to the following examples:

- Balance of Open Access for eB vs Access Control for IA
- Strong DoD IA balanced with industry reality.
- Is the PKI policy supportive of eB objectives and needs? Is it an asset or liability? Can it be executed? If yes, how can it be best executed? If no, then need rationale.
- How will industry respond when policy is implemented? Specifically address use if IECA (and/or ACES). Are there documented concerns by small or small/disadvantaged business or private citizens (etc.) with incorporating PKI like security into DoD processes either from a monetary or ease of use perspective?
- Will the private sector move to class-4-equivalent authentication as natural evolution? If not, why not. If yes, then will it meet our timelines?
- What is resource impact to DoD eB to comply with the policy?
- What are the architectural impacts (e.g. proxy servers to mediate access for trading partners)? How funded by whom, e.g. if proxy servers outside our protected enclave, then someone (project PM?) needs to fund, build and O&M

- What are the security ramifications of using the Defense-in-Depth methodology for eB? That is, should DoD consider implementing a web based access methodology that allows non-DoD users to access web/application servers using Class 2 Certificates or user-ids/passwords and DoD users to access more secure web/application servers BOTH pointed to the same data bases. In this scenario, NO USERS have direct access to the database servers. The web/application servers request data for users from the database servers based on the users' profile.
- Is DoD correct or in error in having ALL DoD networks, data, and systems accessible only via Class 3 or 4 certificates by Oct 2002? Should risk analysis and business cases be used as a basis for determining the acceptable security posture.

Provide recommendations on next actions, including addressing specific policy changes and specific implementation actions.

Deliverable: Output will be an assessment paper and briefing for Mr. Paul Brubaker, Deputy CIO and Mr. Stan Soloway, Director, Defense Reform.